**Topic 3: Intro to SQL**

Top of Form

Bottom of Form

**Content**

**Reading**

[Reading](https://dmacc.blackboard.com/webapps/blackboard/content/listContent.jsp?course_id=_102593_1&content_id=_7286673_1)

SQL

* + Microsoft: docs.microsoft.com
    - [Microsoft SQL documentation](https://docs.microsoft.com/en-us/sql/?view=sql-server-ver15)
  + GeeksforGeeks: geeksforgeeks.com
    - [SQL Tutorial](https://www.geeksforgeeks.org/sql-tutorial/)
  + Tutorialspoint: tutorialspoint.com
    - [SQL Tutorial](https://www.tutorialspoint.com/sql/index.htm)
  + W3Schools
    - [SQL Tutorial](https://www.w3schools.com/sql/)

**SQL Structured Query Language**

[SQL Structured Query Language](https://dmacc.blackboard.com/webapps/blackboard/content/listContent.jsp?course_id=_102593_1&content_id=_7286673_1)

SQL stands for Structured Query Language. It is the standard language used to query, or obtain information, from a database. Many DBMSs use SQL, some have slightly different "flavor" to SQL with very minor differences. It is still important to learn the special features or differences of the DBMS you are using.

MySQL is a free DBMS that you can use. Even MS Access is a database and allows use of SQL.

The basic SQL statement will get all rows and columns from the Table Employees

SELECT \* FROM Employees

You can use more restrictive properties to get only the rows (entries) and columns (fields) you desire:

SELECT EmpID, last\_name, first\_name

FROM Employees

WHERE last\_name LIKE 'R%'

The above query finds employee id, last name and first name for employees whose last name starts with the letter 'R'.

Using more SQL commands, you can organize the information returned as well. Read up on SQL!

**Security threat: SQL Injection Attack (SQLIA)**

[Security threat: SQL Injection Attack (SQLIA)](https://dmacc.blackboard.com/webapps/blackboard/content/listContent.jsp?course_id=_102593_1&content_id=_7286673_1)

You have have heard about security breaches and even the term SQL injection attack.

A basic SQL injection attack uses input that is not sanitized to change underlying SQL code to perform malicious tasks. It might be getting access to a database, gathering sensitive information or just being destructive. Below is a comic talking about a common SQL Injection attack that indicates a name is requested from the user and is just placed in the SQL. Some common tactics to minimize SQLIAs are prepared statements and sanitizing user input. (Google it for more fun info!)

SELECT StudentID FROM Students

WHERE name='Robert'); DROP TABLE Students;--');

The statement below's highlighted portion indicates what the user input was that caused the attack.

|  |
| --- |
| **SELECT StudentID FROM Students WHERE name='Robert'); DROP TABLE Students;--');** |



from :<https://xkcd.com/327/>

When writing code, developers need to keep in mind software safety and security, including such attacks.